13. Appendix C: Build AudioCodes Device (for non-Haystack Sites)

This section explains how to build the AudioCodes devices so it accepts and distributes telephone services. You will need an Ethernet cable to connect to the device.

Login and Password

AudioCodes sets the login and password for this device before they ship it to a customer. They are as follows:

Login: Admin

Password: Admin

CIB Hostnames

The table below contains hostname and rack information for the AudioCode servers you must build. Use it to confirm that all devices are in the MDF and are placed correctly.

Make and Model	Hostname	Rack ID	Rack Unit	Size
AUDIOCODES MEDIANT-1000-MSBG	<sitecode>-vox-gwa-r1	05	38	1 RU
AUDIOCODES MEDIANT-1000-MSBG	<sitecode>-vox-gwa-r2	05	37	1 RU

AudioCodes are used as PSTN gateway for PRI circuits to provide corporate VoIP phone services to allow the site to make and receive external calls.

Access the Audiocodes Device

Via the Avocent Console

1. Attach a console cable between your laptop and the Avocent console.
2. Open a PuTTY session.
3. Login with the Avocent user name and password (admin/avocent) unless someone has updated it.
4. Enter the following commands:

```
--:- / cli->

--:- / cli-> cd /access
--:- access cli-> ls
```

5. Once the cursor reappears, enter the following command to connect to the AudioCodes device: `connect <sitecode>-<hostname>/` Where <sitecode> is the site code for the MDF you are building and hostname is the name of the AudioCodes device.
6. Press the Enter key.
7. Enter the login and password to the AudioCodes device when prompted (Admin/Admin).
8. Continue by following the instructions in the Create IP Address section.

Via a Direct Connection

1. Connect the console cable to the Console port of the device you are configuring. If you are not sure which console cable to use, review Appendix J: Equipment Guide.
2. Open a PuTTY session.
3. Enter the following commands:

```
--:- / cli->

--:- / cli-> cd /access
--:- access cli-> ls
```

4. Once the cursor reappears, enter the following command to connect to the AudioCodes device: `connect <sitecode>-<hostname>/` Where <sitecode> is the site code for the MDF you are building and hostname is the name of the AudioCodes device.
5. Press the Enter key.
6. Enter the login and password to the AudioCodes device when prompted (Admin/Admin).
7. Continue by following the instructions in the Create IP Address section.

Create an IP Address

You must create an IP address for the AudioCodes device, so you can set its hostname. To create an IP address for the primary AudioCodes device (-vox-gwa-r1, eth0-IP), follow this procedure.

Once complete, follow the procedure to create an IP address for the secondary AudioCodes device (-vox-gwa-r2, eth0-IP).

1. Connect to the primary AudioCodes device (-vox-gwa-r1, eth0-IP) via the Avocent console.
2. Enter the following commands. Replace the values in the brackets with the requested values.

```
S #Username: Admin
#Password: Admin

enable
#Password: Admin

config voip
 interface network-if 0
  set ip-address [X.Y.Z.92]
  set prefix-length 29
  set gateway [X.Y.Z.89]
  set primary-dns [DNS IP from NCW]
 exit
exit

config data
 interface VLAN 1
  no service dhcp
 exit
exit
reload now
```

3. Disconnect from the primary AudioCodes device.
4. Connect to the secondary AudioCodes device (-vox-gwa-r2, eth0-IP).
5. Enter the following commands. Replace the values in the brackets with the requested values.

```
#Username: Admin
#Password: Admin

enable
#Password: Admin

configure system
```

```
            hostname <sitecode>-vox-gwa-r#
            exit

config voip
 interface network-if 0
  set ip-address [X.Y.Z.102]
  set prefix-length 29
  set gateway [X.Y.Z.97]
  set primary-dns [DNS IP from NCW]
 exit
exit

config data
 interface VLAN 1
  no service dhcp
 exit
exit
reload now
```

6. Disconnect from the secondary AudioCodes device.

Verify the Firmware

To verify that the AudioCodes device has the appropriate operating system, follow these instructions:

1. Connect to the AudioCodes device.
2. Check the current firmware version for AudioCodes in Appendix B: Current Accepted Image Standard.
3. Run the following command in PuTTY to verify the current firmware show system version.
4. If the firmware listed in Appendix B is not the current firmware, follow steps in AudioCodes section of Appendix A: Troubleshooting to upgrade/downgrade the firmware.

Verify License Keys

License keys are typically installed by the hardware integrator. Complete the following steps to confirm that the licenses are installed, and if not, to install them prior to building the device.

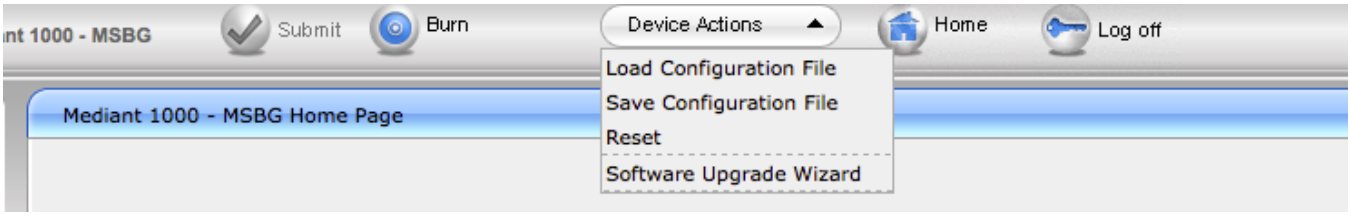
NOTE: Ensure electronic copies of the license key paperwork match the serial number of the device where the license key is being installed.

1. Connect to the device over Ethernet using steps noted above
2. Browse to the device's web management interface using its default IP.
3. Navigate to: Maintenance button > Software Update > Software Upgrade Key.
4. Backup the original factory software key, and save it to the Lab Worksheet for the project.
5. Copy/Paste the new/upgrade license key from the electronically delivered copy of the AudioCodes paperwork to the 'Add a Software Upgrade Key' text box. If you do not have this software key, contact the CIB TPM/Engineer.
6. Click the Burn button at the top of the page.
7. Select Reset Device in the Device Actions menu to reboot the device.

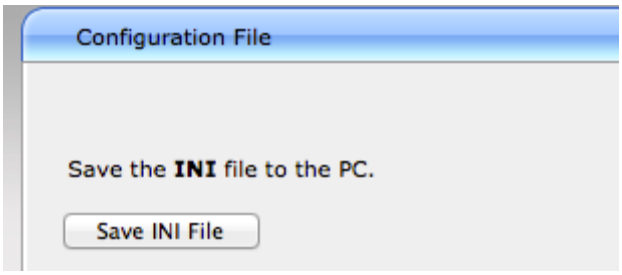
Apply the Config INI

This section assumes that you have completed the build readiness section to create the config INI file.

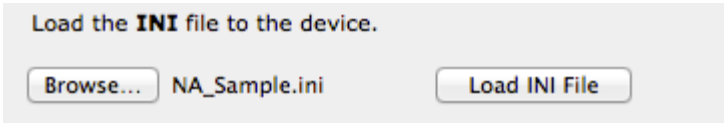
1. Using any web browser, browse to the AudioCodes device through its default IP address,
2. Login using the default user name and password.
3. At the top of the window, Under Device Actions --> Save Configuration File.



4. Save the existing INI configuration file.



5. In that same window, load the INI file came from above script by clicking on Browse, browse to the file, and click on Load INI File.



6. Click OK at the popup window.
7. Wait for a maximum of 10 mins and then refresh the screen. If you get logged out during this process, just log back in using the same credentials as before.
8. If it doesn't come online. Follow the steps in the AudioCodes section of Appendix A: Troubleshooting. You will use a console connection to re-configure the IP. Inform the CIB TPM about this.
9. On the left side of the screen, click the radio button from Basic to Full under the Configuration menu.
10. Click the System menu item.
11. Confirm that the configuration setting for Enablesyslog (System > Syslog Setting >Enablesyslog) is set to Enable.
12. Click the VOIP menu item.
13. Drill to TDM Business settings (TDM>TDM Bus Settings).
14. Confirm that the TDM Bus Clock Source is set to Network.
15. Confirm that the TDM Bus Clock Source is set to Network.
16. Confirm that the TDM Bus PSTN Auto FallBack Clock is set to Enable.
17. Confirm that the TDM Bus PSTN Auto Clock Reverting is set to Enable.
18. Return to the VOIP Menu.
19. Access the Advanced Parameters menu (VOIP >SIP Definitions>Advanced Parameters).
20. Confirm that Disconnect on Broken Connection is set to No.
21. Confirm that Broken Connection Timeout [100 msec] is set to 60000.
22. Return to the VOIP Menu.
23. Access the Proxy and Registration menu (VOIP >SIP Definitions>Proxy & Registration).
24. Confirm that the DNS Query Type is set to NAPTR.
25. Confirm that the Proxy DNS Query Type is set to NAPTR.
26. Exit out of all menus.
27. Save your changes. Do not close the browser window. You will need it to complete the next section.

Verify PRI Activation

Follow these instructions to test that you successfully configured the AudioCodes devices.

1. Connect PRI cables to the first port of AudioCodes gateways. PRI 1 goes to gwa-r1 and PRI 2 goes to gwa-r2. If the carrier didn't leave cables, a straight cat5/6 network cable plays same role. Do not use cross-over cables from carrier's CPE to AudioCodes gateways.
2. Log in to both AudioCodes gateways to verify port status. It should turn to green in 10 seconds. Rest of 3 ports remain in red. If it's not green, match the color with the status listed in the owner's manual. Contact the PM and ask them to call the PRI provider and report the issue.
3. When both PRIs turn to green, in gwa-r1, go to the Status & Diagnostics table, switch the radio button from Basic to Full.
4. Select VOIP Status from the tabs.
5. Select Tel to IP call count.
6. Make few calls to BTN (You can find it from carrier's work order and job sheet). You won't get connected. It makes sure we can see incoming calls from the carrier.
7. Refresh the status. Verify that the value changed in the Number of Attempted Calls field.
    a. If it does not change, contact the PM. Have them call the carrier and report DID porting issue. The carrier can trace call records from their side to locate the problem. If you have the carrier's contact info, feel free to contact them directly.

14. Appendix D: Cisco IOS Upgrade Procedures

A Cisco hardware IOS upgrade is typically included as a service by the hardware integrator. The following steps should still be followed to check the IOS and, if needed, perform an upgrade.

Verify the Current IOS

1. Check the current firmware version in Appendix B: Current Accepted Image Standard.
2. Open PuTTY.
3. Run the `show version` command.

Only proceed to Upload IOS if the operating system shown is incorrect. Otherwise skip to the Apply the Config section.

Upload IOS

1. Get the <redacted> with the Cisco IOS files.
2. Insert the USB drive into the USB port on the front of the device.
3. Enter the following command into PuTTY: `copy usb0:<filename>.img bootflash:` UNLESS you are working with any of these Cisco model numbers (3945, 3750, 3850, and ASR).
   a. If you are working with a 4510 switch, you'll also need to copy the file on the USB drive to the slavebootflash: filesystem to get the file onto the secondary supervisor (`copy usb0:<filename>.img slavebootflash:`).
   b. If you are working with any of these Cisco model numbers (3945, 3750, and ASR), you'll copy to the flash: filesystem instead of bootflash: filesystem. (`copy usb0:<filename>.img flash:`).
4. Press the Enter key on the keyboard to submit the command and copy the file.
5. Enter the following command to view the directory into which you copied the file: `dir bootflash:` and verify that you successfully copied the file to the Cisco device: `dir bootflash:`or `dir slavebootflash:` or `dir flash:` depending on the Cisco device.
6. Enter the following command to run a hash function against the file and ensure that it copied correctly: `verify bootflash:<filename>.img`.

Now you will enter commands so the device can boot from the image you uploaded. The commands are different for different device types.

Cisco <redacted>

Once you complete UPLOAD IOS section above use the following steps to make it a bootable image.

1. Run the following command to un-set any previous boot variables: `show bootvar`. You will see something like the sample below.

```
las10-co-acc-rsw11#sho bootvar
BOOT variable = bootflash:<redacted>-universalk9.SOME.VERSION.NUMBERS.bin,1;
CONFIG_FILE variable does not exist
BOOTLDR variable does not exist
Configuration register is <redacted>

Standby BOOT variable = bootflash:cat4500e-universalk9.SOME.VERSION.NUMBERS.bin,1;
Standby CONFIG_FILE variable does not exist
Standby BOOTLDR variable does not exist
Standby Configuration register is 0x2102
```

2. Use the following command to remove the existing bootflash.bin file and replace it with the new boot file, where `<filename>.bin` is the name of the file you stored on your USB drive.

```
conf t
no boot system flash bootflash:<redacted>-universalk9.SOME.VERSION.NUMBERS.bin
boot system flash bootflash:<filename>.bin
config-register <redacted>
```

```
end
write mem
```

3. Run the following command to verify that the bootvars have updated: `show bootvar`.
4. Run the following command to save the config, and reload the redundant supervisor.

```
copy running-config startup-config
redundancy reload peer
```

5. Wait about five minutes for the program to complete and run the following command: `show redundancy`.
6. Verify that the Peer Processor module's status is `"STANDBY HOT"`. Then verify the image version is correct.
7. Now run the following command: `redundancy force-switchover`.
8. Re-connect to the switch console (or swap your serial console cable over to the other supervisor).
9. Wait five minutes.
10. Run the following command: `show redundancy`. Again, you should see the other Peer Processor module eventually in the `"STANDBY HOT"` state, with the new image version.

This completes the operating system update for the Cisco <redacted>.

Cisco <redacted>

Once you complete UPLOAD IOS section above use the following steps to make it a bootable image.

1. Run the `show bootvar` command to display how the boot variable is configured. You will see output like the example below.

```
ewr3-co-agg-r1#show bootvar
BOOT variable = bootflash:<redacted>-universalk9.SOME.VERSION.NUMBERS.bin,1;
CONFIG_FILE variable does not exist
BOOTLDR variable does not exist
Configuration register is <redacted>
```

2. To remove the `bootflash:<redacted>-universalk9.SOME.VERSION.NUMBERS.bin` lines and add in our new boot file, run the following commands, where `<filename>.bin` is the name of the file you stored on your CorpNet USB drive.

```
conf t
no boot system flash bootflash:<redacted>-universalk9.SOME.VERSION.NUMBERS.bin
boot system flash bootflash:<filename>.bin
config-register <redacted>
end
write mem
```

3. Run the show `bootvar` command again to verify that the boot variable updated. You should now see only `bootflash:<filename>.bin` in the BOOT variable.
4. Run the following command to save the configuration and reload the switch.

```
copy running-config startup-config
reload
```

5. Watch as it comes up on the serial console, or run a ping against it to see when it becomes available again on the network.
6. Log back in.
7. Run the following command to verify the switch is using the correct image version: `show ver`.

This completes the operating system update for the Cisco <redacted>.

Cisco <redacted>

Once you complete the UPLOAD IOS section above use the following steps to make it a bootable image.

1. Run the following command to check the boot image for the device: `show boot`. You will see something like the sample below.

```
ewr3-co-acc-rsw101#show boot
BOOT path-list      : flash:<redacted>.<SOMEVERSION>.bin
Config file         : flash:/config.text
Private Config file : flash:/private-config.text
Enable Break        : no
Manual Boot         : no
HELPER path-list    :
Auto upgrade        : yes
Auto upgrade path   :
NVRAM/Config file
      buffer size:   <redacted>
Timeout for Config
          Download:    0 seconds
Config Download
   via DHCP:       disabled (next boot: disabled).
```

2. Run the following command to upgrade to the uploaded .bin file, where `<filename>.bin` is the name of the file you stored on your CorpNet USB drive.

```
conf t
boot system flash:<filename>.bin
end
write mem
```

3. Run the following command to verify that the system updated the boot variables: `show boot`. If it did not, do not continue, <redacted>.
4. Run the following command to save the configuration and reload the switch.

```
copy running-config startup-config
reload
```

5. Watch as it comes up on the serial console, or run a ping against it to see when it becomes available again on the network.
6. Log back in.
7. Run the following command to verify the switch is using the correct image version: `show version`.

This completes the operating system update for the Cisco <redacted>.

Cisco <redacted>

Once you complete UPLOAD IOS section above use the following steps to make it a bootable image.

1. Run the following command to check the boot image for the device: `show run | incl boot system`. You will see something like the sample below.

```
ewr3-co-acc-v1#show run | incl boot system
boot system flash0:<redacted>.<SOMEVERSION>.bin
```

2. Run the following command to upgrade to <filename>.bin, where `<filename>.bin` is the name of the file you stored on your CorpNet USB drive.

```
conf t
no boot system flash0:<redacted>.SOMEVERSION.bin
boot system flash:<filename>.bin
end
write mem
```

3. Run the following command to save the configuration and reload the switch.

```
copy running-config startup-config
reload
```

4. Watch as it comes up on the serial console, or run a ping against it to see when it becomes available again on the network.
5. Log back in.
6. Run the following command to verify the switch is using the correct image version: `show ver`.

This completes the operating system update for the Cisco <redacted>.

Cisco <redacted>

Once you complete <redacted> section above use the following steps to make it a bootable image.

1. Run the following command to check the boot image for the device: `show boot`. You will see something like the sample below.

```
bos12-co-acc-v1#sho bootvar
BOOT variable = flash:<redacted>.SOME.VERSION.NUMBERS.bin,12;
CONFIG_FILE variable does not exist
BOOTLDR variable does not exist
Configuration register is <redacted>

Standby not ready to show bootvar
```

2. To remove the `bootflash:<redacted>.SOME.VERSION.NUMBERS.bin` lines and add in our new boot file, run the following commands, where `<filename>.bin` is the name of the file you stored on your CorpNet USB drive.

```
conf t
no boot system flash flash:<redacted>.SOME.VERSION.NUMBERS.bin
boot system flash flash:<filename>.bin
config-register <redacted>
end
write mem
```

3. Run the show `bootvar` command again to verify that the boot variable updated. You should now see only `bootflash:<filename>.bin` in the BOOT variable.
4. Run the following command to save the configuration and reload the switch.

```
copy running-config startup-config
reload
```

5. Watch as it comes up on the serial console, or run a ping against it to see when it becomes available again on the network.
6. Log back in.
7. Run the following command to verify the switch is using the correct image version: `show ver`.

This completes the operating system update for the Cisco <redacted>.